UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,002	07/05/2001	Mark J. McArdle	002114.P020	5144

8791 7590 12/08/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
MAURO JR, THOMAS J	

ART UNIT	PAPER NUMBER
2143	

DATE MAILED: 12/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/900,002	MCARDLE ET AL.	
	Examiner	Art Unit	
	Thomas J. Mauro Jr.	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are pending and are presented for examination. A formal action on the merits of claims 1-21 follows.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 1, 7, 12 and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Xie et al. (U.S. 6,772,347).

With respect to claim 1, Xie teaches a computerized method for restricting network access by applications comprising:

detecting a network access request from an application **[Xie -- Col. 4 lines 46-57 – The firewall engine receives a packet and places the packet in memory]**;

examining an application policy file to determine if the application is authorized to access the network **[Xie -- Col. 4 lines 50-67 – Col. 5 lines 1-22, Col. 5 lines 30-39 and lines 51-57 and Col. 6 lines 48-62 – Rules, i.e. policy file, is examined to determine if a given application, identified by its port number, is allowed to access the network, i.e. pass through the firewall]**; and

blocking access to the network if the application is not authorized to access the network **[Xie -- Col. 5 lines 23-29 and Col. 5 lines 45-67 – Col. 6 lines 1-5 – Based upon rules, access to network can be denied, i.e. blocked, if the rules determine application, identified by port number, is not allowed]**.

With respect to claim 7, Xie teaches a computer-readable medium having executable instructions **[Xie -- Col. 3 lines 52-67 – Col. 4 lines 1-11 – Software, i.e. executable instructions, stored in memory]**. The remaining limitations in claim 7 are similar to the limitations recited in claim 1 above. Therefore, claim 7 is rejected under the same rationale.

With respect to claim 12, Xie teaches a computer system comprising:

a processing unit;

a memory coupled to the processing unit through a bus; and

a network interface coupled to the processing unit through the bus and further operable for coupling to a network **[Xie -- Figures 1, 2A, 2B, Col. 1 lines 55-67 – Col. 2 lines 1-28 and Col. 3 lines 52-67 – Col. 4 lines 1-11 – System includes a processor, i.e. CPU, memory, i.e. RAM, and network interface to access the network all connected through a bus]**.
The remaining limitations in claim 12 are similar to the limitations recited in claim 1 above. Therefore, claim 12 is rejected under the same rationale.

With respect to claim 18, Xie teaches a computer-readable medium having stored thereon an application policy data structure comprising:

an application identifier field containing data identifying an application **[Xie -- Figure 3 and Col. 4 lines 13-16 and lines 28-42 and Col. 5 lines 34-39 – Application identifier field, i.e. source and destination port number, identified application]**;

a network identifier field containing data identifying an entity that is accessible by the application identified by the application identifier field **[Xie -- Figure 3 and Col. 4 lines 13-16 and lines 28-42 and Col. 5 lines 34-39 – Source/Destination IP addresses define network entities which the application can access]**; and

an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field **[Xie -- Figure 3 and Col. 4 lines 13-16 and lines 28-42 and Col. 5 lines 23-29 and lines 34-39 – Status register, i.e. flag, specifies what action is to be taken if the rule is matched, i.e. allow or deny]**.

4. Claims 1-3, 5-9, 11-14 and 16-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Coss et al. (U.S. 6,154,775).

With respect to claim 1, Coss teaches a computerized method for restricting network access by applications comprising:

detecting a network access request from an application **[Coss -- Figure 5A, 5B and Col. 6 lines 19-30 – IP packets are received by the firewall at an interface]**;

examining an application policy file to determine if the application is authorized to access the network **[Coss -- Figures 3 and 4, Col. 4 lines 4-67 and Col. 5 lines 60-67 – Col. 6 lines 1-2 and lines 38-51 – Security policies access rules are examined to determine if an application, i.e. service, is authorized to access the network]**; and

blocking access to the network if the application is not authorized to access the network **[Coss -- Figures 3 and 4, Col. 4 lines 4-67 – Based upon access rules, packet will either be passed or dropped, i.e. blocked]**.

With respect to claim 2, Coss further teaches the method further comprising:

determining a network resource requested by the application, examining the application policy file to determine if the application is authorized to access the network resource, and, allowing access to the network resource if the application is authorized to access the network resource **[Coss -- Figures 3 and 4, Col. 4 lines 4-67 and Col. 6 lines 29-60 and Col. 7 lines 4-9 – IP packets received at firewall are examined to determine network resource, i.e. destination IP address/port including service. Security profile access rules are examined to determined if the rules specify to drop or pass the packets; thereby, allowing packets specified in an access rule for the network resource, i.e. IP address]**.

With respect to claim 3, Coss further teaches the method further comprising:

determining a type of network access requested by the application, examining the application policy file to determine if the application is authorized for the type of network access requested, and, allowing the type of network access requested if the application is authorized for

the type of network access requested **[Coss -- Figures 3 and 4, Col. 4 lines 4-67 and Col. 6 lines 29-60 and Col. 7 lines 4-9 – IP packets received at firewall are examined to determine type of network access requested, i.e. TELNET, FTP, MAIL, etc.. Security profile access rules are examined to determined if the rules specify to drop or pass the packets; thereby, allowing packets specified in an access rule for the particular type of access, i.e. FTP – Pass (Figure 3)]**.

With respect to claim 5, Coss further teaches the method further comprising:

determining if the application is allowed access to the network based on an application identifier in the network access request **[Coss -- Figure 3, Col. 4 lines 4-69 and Col. 5 lines 60-67 – Col. 6 lines 1-2 – Application is identified in the request via the source port number which identifies the application from which the request was initiated]**.

With respect to claim 6, Coss further teaches wherein the method is performed on a client computer on which the application is executing **[Coss -- Figure 1, Col. 3 lines 37-57 and Col. 10 lines 25-32 – Filtering of network access via access rules can be performed on a client computer/device which is running an application]**.

With respect to claim 7, Coss teaches a computer-readable medium having executable instructions **[Coss -- Col. 3 lines 25-35 – Computer software, i.e. instructions]**. The remaining limitations in claim 7 are similar to the limitations recited in claim 1 above. Therefore, claim 7 is rejected under the same rationale.

With respect to claims 8, 9 and 11, these are computer-readable medium claims corresponding to the method claimed in claims 2, 3 and 5 above. They have similar limitations; therefore, claims 8, 9 and 11 are rejected under the same rationale.

With respect to claim 12, Coss teaches a computer system comprising:

a processing unit;

a memory coupled to the processing unit through a bus; and

a network interface coupled to the processing unit through the bus and further operable for coupling to a network **[Coss -- Figures 1, and 2, Col. 3 lines 43-67 and Col. 11 lines 35-40 – Computer systems connected to network includes processor and memory, inherently connected by bus]**.

The remaining limitations in claim 12 are similar to the limitations recited in claim 1 above. Therefore, claim 12 is rejected under the same rationale.

With respect to claims 13, 14, 16 and 17, these are system claims corresponding to the method claimed in claims 2, 3, 5 and 6 above. They have similar limitations; therefore, claims 13, 14, 16 and 17 are rejected under the same rationale.

With respect to claim 18, Coss teaches a computer-readable medium having stored thereon an application policy data structure comprising:

an application identifier field containing data identifying an application **[Coss -- Figures 3 and 4, Col. 4 lines 4-19 and lines 40-67 and Col. 5 lines 60-67 – Col. 6 lines 1-2 – Service information along with source/destination port identifiers, serve to identify the application, i.e. FTP, TELNET, MAIL, etc.]**;

a network identifier field containing data identifying an entity that is accessible by the application identified by the application identifier field **[Coss -- Figure 3, Col. 4 lines 4-19 and lines 27-45 and Col. 5 lines 60-67 – Source/Destination IP addresses define network entities which the application can access]**; and

an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field **[Coss -- Figures 3 and 4, Col. 4 lines 4-67 – Access rules contain a field specifying an action of whether to pass, drop or proxy the packets]**.

With respect to claim 19, Coss further teaches the computer-readable medium further comprising:

an additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field **[Coss -- Col. 4 lines 4-67 – Col. 5 lines 1-35 – The access rules categories can specify types of access to a particular entity including date/time controlled access and tunneling access requirements, requiring a tunnel to be set up for certain destination entities]**.

With respect to claim 20, Coss further teaches the computer-readable medium further comprising:

a response field containing data specifying an action to be performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed **[Coss -- Figures 3, 4 and Col. 4 lines 4-67 – Col. 5 lines 1-35 – Access rules categories specify an action to be performed, including pass, proxy or drop the packets and additionally include alarm conditions for notification]**.

With respect to claim 21, Coss further teaches the computer-readable medium wherein the entity is a network resource **[Coss -- Figure 3, Col. 4 lines 4-37 and Col. 6 lines 60-67 – Entity is a network resource, i.e. server, identified by an IP address]**.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4, 10 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coss et al. (U.S. 6,154,775).

Regarding claim 4, Coss teaches the invention substantially as claimed, including updating the application policy file **[Coss -- Col. 8 lines 28-59 – Updated rules, i.e. dynamic rules, can be loaded at any time by a trusted part; thereby updating the security policy access rules]**, but fail to explicitly teach re-evaluating applications currently executing against the updated policy file.

It is notoriously well known in the art and obvious that if a process or method can be executed a first time, it can likewise be duplicated and executed again.

Thus, it would have been obvious to a person of ordinary skill in the art that as access rules change, current connections in place before the new access rules should be re-checked to determine if, due to the new rules, connections should be dropped, as this would provide better overall security and system protection from attacks.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the re-evaluation of applications currently executing, i.e. accessing the network, as access rules are modified and changed into the invention of Coss, in order to provide the network with greater security and protection from attacks as new threats and vulnerabilities arise which previously were not a problem.

Regarding claim 10, this is a computer-readable medium claim corresponding to the method claimed in claim 4 above. It has similar limitations; therefore, claim 10 is rejected under the same rationale.

Regarding claim 15, this is a system claim corresponding to the method claimed in claim 4 above. It has similar limitations; therefore, claim 15 is rejected under the same rationale.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Hericourt (U.S. 6,792,461) discloses a system for managing data by an application level protocol including traffic policing.

- Moses et al. (U.S. 6,499,110) discloses a method for facilitating information security policy controls using multiple security engines.

- Nagar et al. (U.S. 6,604,143) discloses scalable proxy servers with plug-in filters.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas J. Mauro Jr. whose telephone number is 571-272-3917. The examiner can normally be reached on M-F 8:00a.m. - 4:30p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on 571-272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TJM
November 26, 2004

Primary Examiner
Art Unit 2143
William C. Vaughn, Jr.